GDPR for regnskapsførere

Ny personvernlov fra mai 2018 - GDPR

- EU-forordning som etter EØS avtalen skal implementeres i norsk lov
- Vil påvirke behandlingen av personopplysninger i regnskapsførervirksomhet
- Påvirker også kundene og underleverandørene
- Regnskap Norge mener at de fleste regnskapsførervirksomheter ikke vil trenge et personvernombud
- Anbefalt å lese seg opp på regelverket

Viktigste endringer

- Tydeligere aktivitetskrav for bedriftene
- Omfattende ansvarliggjøring når avvik oppstår
- Sanksjoner

Større krav til beskyttelse av borgerne i et digitalt samfunn

- Sikre borgerne kontroll over egne personopplysninger
- Samtykke til bruk
- Nekte behandling
- Rett til å bli glemt
- Lovlig, rettferdig og transparent behandling
- Personopplysninger kan misbrukes av mange
- På mange forskjellige måter

Hva er personvernopplysninger?

- Opplysninger eller vurderinger som kan knyttes til enkeltpersoner
- Navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform og fødselsnummer
- Sensitive personopplysninger – rase og etnisk bakgrunn, religiøs, politisk eller filosofisk oppfatning, helse, seksuelle forhold, medlemskap i fagforbund, mistenkt, siktet eller tiltalt for straffbar handling
- Behandling av sensitive personopplysninger er som utgangspunkt forbudt med visse unntak
- Personnummer er ikke sensitive personopplysninger i denne sammenheng

Behandlingsansvarlig og databehandler

- Behandler personopplysninger på vegne av kunder – databehandler
- Kundene er behandlingsansvarlig
- Behandlingsansvarlig bestemmer formålet med behandlingen
- Personopplysninger om egne ansatte – behandlingsansvarlig
- Regnskapsførere, revisorer og advokater er som regel databehandlere
- Ovenfor egne ansatte er de behandlingsansvarlig
- Behandlingsansvarlig kan sette ut behandlingen til en databehandler men beholder selv allikevel ansvaret
- Databehandleren skal imidlertid varsle dersom kunden ikke følger loven
- Kan bli stilt til ansvar ved manglende varsling

Fremgangsmåte for implementering

- Starte med å identifisere alle personopplysninger som virksomheten behandler
- Både digitalt og manuelt
- Strukturerte personopplysninger er lettere å håndtere – sørg for struktur
- Ustrukturerte personopplysninger er vanskeligere å kartlegge – ikke legg inn personopplysninger i ulike ustrukturerte systemer hvor dette ikke er strengt nødvendig
- Saml personopplysningene mest mulig i færrest mulige systemer
- Krav om innebygd personvern i systemets oppbygging i loven
- Logiske, strukturerte og krypterte databaser kan inngå i dette kravet
- Letter også flyttingen av personopplysninger
- Fjern personopplysninger som ikke lenger har et reelt formål

Klassifisering av personopplysninger

- Klassifisere ordinære og sensitive personopplysninger
- For å sikre at det etableres tilstrekkelig intern kontroll
- Behandling av sensitive personopplysninger er som utgangspunkt forbudt
- Begrunnelse for slik behandling må komme tydelig frem - dokumenteres

Formålet med behandlingen

- Angi alltid formålet med behandlingen av personopplysninger
- Om formålet endrer må det innhentes nytt samtykke
- Ellers skal opplysningene slettes
- Annet formål en det personen har gitt tillatelse til
- Svært viktige handlinger etter loven!

Oppbevaring og behandling

- Først – oversikt over hvilke personopplysninger som behandles
- Så – hvorfor de behandles
- Deretter hvor de prosesseres – hvilke systemer
- Så hvor de oppbevares
- Som utgangspunkt oppbevaring innenfor EØS – unntak kan gis av Datatilsynet
- Oppbevaring i egen organisasjon eller hos underleverandør
- Er ansvarlig for hele kjeden som behandlingsansvarlig

Risikovurdering

- Må vurdere risikoen for urettmessig eksponering og bruk av personopplysninger
- Må vurdere konsekvensene hvis data blir eksponert eller misbrukt
- Må vurdere opplysningenes art, omfang og formål
- Kalles i loven konsekvensanalyse

Konsekvensanalyse

Kan gjøres i fire trinn:

1. Kartlegge informasjonssystemene og hvilke opplysninger som behandles i disse
2. Identifisere risiko knyttet til personopplysninger
3. Identifisering og anbefaling av tiltak
4. Dokumentasjon

- Kan være lurt å grupper like typer data som har lik risiko og krever lik beskyttelse
- Personopplysninger vil kunne ha svært forskjellig risiko for eksponering og misbruk

Internkontroll

Må baseres på risiko- og konsekvensanalysen og skal ha følgende målsetning:

1. Konfidensialitet – sikre at kun autoriserte brukere har tilgang
2. Tilgjengelighet – sikre at opplysningene er tilgjengelig for autoriserte personer ved behov
3. Integritet – sikre nøyaktighet og fullstendighet, sikkerhet mot uautoriserte endringer og sikre sporbarhet av endringer

- Mye løses ved gode rutiner rundt datasikkerhet!

Etablering av avtale verk

- Det skal foreligge et avtaleverk i bunn
- Mellom personene og virksomhetene som behandler personopplysninger
- Og mellom behandleren og eventuelle databehandlere
- Det skal foreligge avtaler i alle ledd – hele kjeden
- For eksempel mellom kunde og bedrift, bedriften og regnskapsfører, regnskapsfører og systemleverandør, systemleverandør og driftsleverandør
- En avtale mellom kunde og bedrift kan lettes formuleres som et digitalt samtykke formular

Personvernombud

- Som utgangspunkt antas det at det ikke er nødvendig med personvernombud i regnskapsbedrifter
- Kan frivillig etablere et ombud – da helst ved behandling av store datamengder for mange kunder
- Driver ikke med systematisk motonitorering i stor skala
- Driver ikke med systematisk behandling av sensitive opplysninger
- Frivillig etablering av personvernombud vil imidlertid kunne sikre en god behandling av personopplysninger

Samtykke

- Ikke alle opplysninger trenger samtykke – for eksempler opplysninger hjemlet i lov ved ansettelsesforhold eller for ivaretakelse av offentlige oppgaver
- Andre opplysninger krever som hovedregel samtykke
- Behandlingsansvarlig plikter da å dokumentere at samtykke er gitt
- Personen skal informeres om formåler og sine rettigheter
- Bedriften bør bruke standardisert informasjon
- Personen kan trekke tilbake samtykket når som helst
- Personen kan nekte behandling og «kreve å bli glemt»
- Må ha rutiner for dette

Innsynsrett

- En person kan kreve innsyn i hvilke personopplysninger som er samlet og formålet med opplysningene
- Må være begrunnet – ikke helt grunnløst
- Må ha effektive rutiner for å sammenstille opplysninger fra alle kilder for å ivareta denne innsynsretten
- En person har også rett til å korrigere sine personopplysninger

Dataportabilitet

- En person kan kreve at elektronisk registrerte personopplysninger skal flyttes fra behandlingsansvarlig A til behandlingsansvarlig B
- I et alminnelig format som er maskinleselig
- Kan ikke kreves dersom ny mottaker ikke kan behandle formatet

Rutiner for sletting

- Retten til å bli glemt
- Bedriften må ha rutiner for sletting av alle relevante personopplysninger
- Uten ugrunnet opphold
- Også sikkerhetskopier
- Kravet gjelder ikke for oppbevaringspliktige regnskapsopplysninger – kan ikke kreves slettet

Varslingsplikt

- Ved brudd på personopplysningssikkerheten skal Datatilsynet varsles umiddelbart
- Senest innen 72 timer
- Ved risiko for eksponering
- Om regnskapsfører oppdager brudd må kunden straks informeres som så igjen må varsle Datatilsynet
- Er risikoen høy for personen skal også personen varsles
- Viktig med gode varslingsrutiner og oppdaterte varslingslister

Bransjenorm

- Bransjene kan etablere en norm – for eksempel for regnskapsførere, revisorer og advokater
- Dette vil være en god hjelp får å få en forståelse for hva som er viktig i de nye og svært omfattende reglene for din bransje
- En bransjenorm/atferdsnorm for regnskapsbransjen er laget (07.05.18) men ennå ikke godkjent av datatilsynet
- Da blir det hele «litt» enklere!

Bransjenorm

Forslag til bransjenorm av 7. mai 2018

- Utarbeidet av bransjestandardutvalget til Regnskap Norge, Økonomiforbundet og Revisorforeningen
- Formål – å beskrive rutiner og intern kontroll for å sikre etterlevelse av personvernreglene ved utførelse av regnskapsoppdrag mv.
- Som databehandler for kunder
- Ikke rettet mot regnskapsvirksomhetens rolle som behandlingsansvarlig

Regnskapsbransjens rolle

- Regnskapsbransjen behandler mange personopplysninger implisitt i sitt arbeid for kunder
- Derfor viktig med god intern kontroll ved behandlingen for god etterlevelse av personvernreglene
- Regnskapsførerloven § 2 – skal utføre sine oppdrag i samsvar med denne, i medhold av lov og i henhold til god regnskapsførerskikk
- Etter §10 i regnskapsførerloven har alle ansatt taushetsplikt om alt de under sin virksomhet for kjennskap til – med mindre det er gitt unntak i lov eller den det gjelder samtykker
- Kan ikke bruke opplysningene i egen (annen) virksomhet eller i tjeneste eller arbeid for andre
- GRFS gir føringer om krav til intern kontroll, rutiner, konfidensialitet og sikring som er relevant i denne sammenheng

Avgrensninger

- Oppdragsavtalen avgrenser oppdraget og avgrenser samtidig de personopplysninger som er nødvendig i tråd med dette
- Det skal inngås en databehandleravtale i tråd med dette som spesifikt omhandler og avgrenser hvilke personopplysninger som kan deles/behandles
- Denne kan implementeres i oppdragsavtalen eller lages separat

Roller

- Behandlingsansvarlig/kunden har de primære pliktene etter personvernlovgivningen
- Kan benytte regnskapsførervirksomheten til å ivareta noen av disse pliktene gjennom oppdragsavtale og databehandleravtale
- Regnskapsvirksomheten vil ha selvstendige plikter i henhold til dette
- Den registrerte skal forholde seg til oppdragsgiver
- Kan ikke henvende seg til databehandler med mindre det foreligger spesifikk avtale om dette

Kartlegging av personopplysninger

- Det skal foreligge en oversikt over alle personopplysninger som behandles på vegne av oppdragsgiver
- Ved lik behandling kan denne dokumentasjonen utarbeides under ett
- Den generelle dokumentasjonen skal kompletteres med særskilte forhold for oppdragsgiver med avvikende formål og behandling
- Ved ulik behandling f eks ved bruk av forskjellige lønnssystemer må dokumentasjonen tilpasses og beskrives spesifikt for de ulike systemer

Formål med behandling av personopplysninger

- I hovedsak for å assistere oppdragsgiver med sine plikter i forbindelse med regnskap, lønn, skatt og avgift og rådgivning
- Registrere lønnsgrunnlag
- Utarbeide lønnsdokumentasjon
- Utarbeide grunnlag for utbetaling av lønn, feriepenger, skattetrekk og arbeidsgiveravgift
- Utarbeidelse og innsending av offentlige oppgaver for oppdragsgiver
- Korrekt bokføring av lønnsrelaterte regnskapsopplysninger
- Innrapportering til NAV, SSB og andre interessenter med lovhjemlet krav på opplysninger
- Skal ikke brukes til andre formål – mindre unntak for sammenstilte og anonymiserte opplysninger

Åpenhet i behandlingen

- Personopplysninger skal behandles på en lovlig, rettferdig og åpen måte
- Virksomheten skal kunne gjøre rede for hvordan behandlingen skjer i egen virksomhet og hos underleverandører
- Kan skje muntlig og ved fremleggelse av skriftlig dokumentasjon – rutinebeskrivelser, prosedyrer, flytskjema mv.
- Ikke nødvendig å fremlegge detaljer med mindre dette er absolutt nødvendig for forståelsen

Personvernkontakt og personvernombud

- Det skal pekes ut en personvernkontakt
- Skal ivareta regelverket rundt personopplysninger og være kontaktperson for eksterne parter
- Skal være daglig leder eller utpekt av denne
- Skal ha gjennomført opplæring og oppdatere sin kompetanse
- Regnskapsførervirksomheter trenger normalt ikke personvernombud
- Unntak ved oppdrag for offentlige myndigheter og organer hvor en behandler særskilte kategorier personopplysninger i stor skala
- Unntak dersom behandlingsansvarlig må ha personombud og databehandler mottar opplysninger som har forbindelse med dette
- Kontaktopplysninger om personvernombud skal offentliggjøres og meddeles Datatilsynet

Vurdering av personvernkonsekvenser og risikovurdering

- Vurdering av personvernkonsekvenser – DPIA
- Skal utarbeides av behandlingsansvarlig i tilfeller med høy risiko
- Regnskapsførervirksomheten kan bistå i dette arbeidet etter avtale
- Risikovurderingen skal ellers gjennomføres sammen med annen risikovurdering i regnskapsførervirksomheten for å sikre en helhetlig tilnærming
- Skal inneholde en vurdering av risiko for intern eksponering og eksponering hos eksterne system og/eller driftsleverandører
- Også risikoen for mulig eksponering overfor uvedkommende utenfor behandlingsmiljøet skal vurderes
- Risikovurderingen skal være skriftlig, oppdatert og tilgjengelig for tilsynsmyndigheten
- Bransjestandardutvalget har laget en mal for oppbyggingen

Særlige kategorier av personopplysninger

- Regnskapsførervirksomheten behandler i enkelte tilfeller særskilte personopplysninger – f eks tilknytning til fagforeninger, trossamfunn og helseopplysninger
- Dette er i utgangspunktet forbudt
- Behandling av slike opplysninger for rapporteringspliktige formål er tillatt
- Virksomheten skal ha egne konsultasjoner med oppdragsgiver om behandling av slike personopplysninger og nødvendigheten av å behandle disse
- Disse konsultasjonene skal være dokumentert, inneholde en risikovurdering og en beskrivelse av intern kontroll
- Skal ha høy oppmerksomhet og god kontroll
- Tilgangen skal holdes på et minimum

Rutiner og innebygd personvern

- Tilgang skal kun gis til personer i virksomheten med et berettiget behov for opplysningene for å ivareta sine plikter i henhold til oppdragsavtalen, gjeldende lovkrav og god regnskapsførerskikk
- NBS 1 om sikring av regnskapsmateriale skal brukes som veiledning
- Skal sikre tilstrekkelige logiske og fysiske sikkerhetstiltak i hele behandlerløpet
- Skal sikre konfidensialitet, integritet og tilgjengelighet
- Forskjell på små og store virksomheter – forskjellige behov
- Mangel på innebygd personvern må kompenseres med internkontroll inntil personvernet er innebygd
- Om systemene ikke har et tilstrekkelig innebygd personvern må systemet byttes
- Flytte opplysninger fra ustrukturerte til strukturerte arkiver

Dokumentasjon av oppbevaringssted

- To dimensjoner
- 1. Land – skal ha dokumentasjon på fysisk oppbevaringssted for alle ledd frem til endelig sted
- Tilstrekkelig med land og leverandør i dokumentasjonen
- Om dette ikke er mulig må behandlingen stoppes inntil dette ar avklart

- 2. System – hvilket system personopplysningene blir oppbevart i
- Nødvendig for effektivt innsyn og dataportabilitet

Avtaleverk mellom behandlingsansvarlig og databehandler

- Det skal foreligge en databehandleravtale mellom oppdragsgiver og regnskapsførervirksomheten
- Selvstendig eller som en del av oppdragsavtalen
- Skal være skriftlig og signert av partene
- Det skal også foreligge en tilsvarende avtale med alle underleverandører
- Underleverandørene skal ha en tilsvarende avtale med sine eventuelle underleverandører
- Oppdragsgiver og regnskapsførervirksomheten skal ha dokumentasjon av alle databehandlere som er involvert i oppdraget

Rutiner for samtykke, motsettelse av behandling, innsyn og retting

- Oppdragsgiver skal innhente samtykke til behandling av personopplysninger hvor dette kreves
- Regnskapsførervirksomheten skal varsle oppdragsgiver dersom de er eller blir klar over at dette samtykket mangler
- Det er kun oppdragsgiver som kan instruere regnskapsførervirksomheten
- Ikke behandling, krav om innsyn og retting må tas opp med behandlingsansvarlig/oppdragsgiver med mindre det foreligger avtale om annet
- Regnskapsførervirksomheten skal varsle oppdragsgiver om mangler ved behandlingen umiddelbart
- Regnskapsfører skal ikke gi innsyn i registrerte opplysninger til den registrerte uten godkjenning fra oppdragsgiver med mindre det foreligger en direkte juridisk rett til innsyn

Rutiner for dataportabilitet

- Den registrerte kan kreve elektronisk oppbevarte personopplysninger overført elektronisk til annen behandlingsansvarlig hvis denne kan lese opplysningene elektronisk
- Kan etter avtale tilrettelegge for dataportabilitet med oppdragsgiver gjennom sin kunnskap
- En samlet programmert aktivitet eller en sammenstilling av opplysninger manuelt tilpasset hva en kan håndtere
- Kan ikke oversende opplysninger uten at oppdragsgiver har godkjent dette
- Oppdragsgiver kan instruere regnskapsfører om overflytting ved bytte av regnskapsfører ved opphør av oppdragsavtalen etter de samme prinsipper

Rutiner for endring av formål

- Oppdragsgiver bestemmer formålet med behandling av personopplysninger
- Endringer i eller utvidelse av formålet må reflekteres i endret oppdragsavtale, databehandleravtale eller nye avtaler
- Oppdragsgiver skal umiddelbart varsles dersom formålet ikke lenger er i tråd med personopplysningslovgivningen – f eks dersom det mangler samtykke for nye formål

Rutiner for sletting av personopplysninger

- Oppdragsgiver har ansvar for sletting når formålet for behandling ikke lenger er tilstede
- Regnskapsførervirksomheten skal kun slette opplysninger etter avtale eller instruks fra oppdragsgiver
- Kan bli enige om faste slettingsrutiner
- Oppdragsgiver skal varsles dersom en blir klar over at oppdragsgiver ikke følger reglene for sletting
- Kan ikke oppbevare personopplysninger etter slettetidspunktet med mindre dette er avtalt med oppdragsgiver og formålet er gyldig
- Må ha rutiner for sletting etter utløpet av pliktige oppbevaringsperioder
- Må slette over alt – originalt arkiv, andre reproduksjoner og sikkerhetskopier etter bokføringsforskriften
- Sletting skal ikke utføres hvis opplysningene er nødvendig for å sikre lovbestemte oppbevaringskrav

Rutiner for avvikshåndtering og rapportering

- Oppdragsgiver skal varsles umiddelbart dersom en blir kjent med at personopplysningene behandles i strid med personvernloven
- Skal også varsle oppdragsgiver umiddelbart dersom en blir klar over at personopplysninger er på avveie

Dokumentasjon av prosedyrer og interkontroll

- Personvernet skal bygges inn i daglige rutiner og prosedyrer der hvor personopplysninger behandles
- Alle flytskjema, rutinebeskrivelser og prosedyrer som har relevans skal være skriftlige og lett til tilgjengelig
- Dokumentasjonen skal underbygge krav om åpenhet i behandlingen
- Dokumentasjonen rundt prosedyrer og intern kontroll skal oppdateres når det har skjedd endringer som gjør at dette er nødvendig

Kontroll av etterlevelsen av atferdsnormen

- Fremtidige kontroller av medlemmer som er underlagt bransjeorganisasjonene vil inkludere etterlevelsen av atferdsnormen
- Finanstilsynet vil sikkert også ha et ord med i laget i denne sammenheng

Takk for oppmerksomheten!

Kontaktdetaljer:

Jan Bangen

Web: www.bondelaget.no

Epost: jan.bangen@bondelaget.no

Mobil: 958 93 917